Authenticated cryptographic key exchange in digital subscriber network - using preliminary phase of multiplication in finite galois field with random number selection for public key

Patent Number: CH678134
Publication date: 1991-07-31
Inventor(s): GUENTHER CHRISTOPH DR
Applicant(s):: ASCOM RADIOCOM AG
Requested Patent: ☐ CH678134
Application Number: CH19890000105 19890113
Priority Number(s): CH19890000105 19890113
IPC Classification: H04K1/02 ; H04L9/28
EC Classification: H04L9/32, H04L9/08D2
Equivalents:

Abstract

The subscribers (A,B etc.) are connected to a key distribution centre (SVZ) for the preauthentication phase in which they signal their identities in accordance with the El Gamal scheme. The centre selects a Galois field GF(q) and a primitive (alpha) which is raised to the power of a negative random number (x) to form the public part of the key.
In the following exchange phase two subscribers produce a common secret key by a modified Diffie-Hellmann method.
ADVANTAGE - Flexible enough for extension to new and individually distinguishable subscribers, and requires little memory capacity.

CH 678134 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(11) CH 678134 A5

(51) Int. Cl.[5]: H 04 K 1/02
H 04 L 9/28

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(21) Gesuchsnummer: 105/89

(22) Anmeldungsdatum: 13.01.1989

(24) Patent erteilt: 31.07.1991

(45) Patentschrift veröffentlicht: 31.07.1991

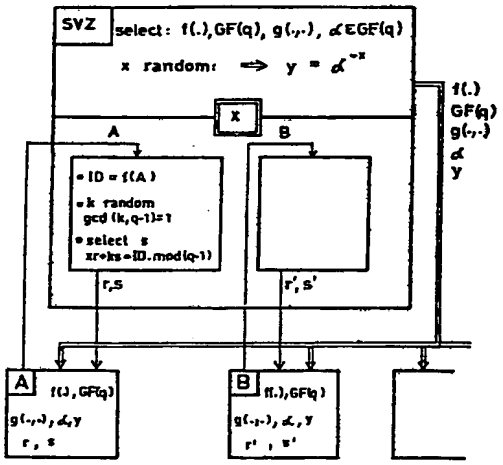
(73) Inhaber:
Ascom Radiocom AG, Solothurn

(72) Erfinder:
Günther, Christoph, Dr., Fislisbach

(74) Vertreter:
ASEA Brown Boveri AG, Baden

(54) Verfahren zum authentifizierten Schlüsselaustausch.

(57) Der erfindungsgemässe Schlüsselaustausch findet in einem Netz mit einer Schlüsselverteilzentrale SVZ und mehreren Benutzern A, B, ... statt und weist zwei Phasen auf, nämlich eine Präauthentifikationsphase und eine Schlüsselaustauschphase. In der Präauthentifikationsphase kommt jeder Benutzer A, B, ... zur Schlüsselverteilzentrale SVZ und lässt sich seine Identität mit dem ElGamal Schema signieren. In der nachfolgenden Schlüsselaustauschphase erzeugen zwei Benutzer A und B einen gemeinsamen Geheimschlüssel z nach einem abgeänderten Diffie-Hellmann Verfahren.



Beschreibung

Technisches Gebiet

Die Erfindung betrifft ein Verfahren zum authentifizierten Schlüsselaustausch in einem Netz mit einer Schlüsselverteilzentrale und mehreren Teilnehmern.

Stand der Technik

Verfahren zur Erzeugung von authentifizierten Geheimschlüsseln werden z.B. in der europäischen Patentanmeldung EP-A 0 307 627 und in der deutschen Auslegeschrift DE-A 3 915 262 beschrieben.

Das erste der beiden Verfahren führt die Authentifikation über das öffentliche Telefonnetz durch und ist entsprechend nicht für alle Anwendungen gleichermassen geeignet. Das zweite Verfahren verwendet eine präauthentifizierte Liste von öffentlichen Teilnehmerschlüsseln und ist für den automatischen Betrieb entworfen worden. Bei der Aufnahme einer Verbindung muss jedoch der öffentliche Teilnehmerschlüssel jeweils aus der präauthentifizierten Liste gelesen werden. Dabei gibt es zwei Möglichkeiten: Entweder wird die Liste in jedem Gerät gespeichert, was bei grossen Netzen viel Speicherplatz (proportional zur Teilnehmerzahl) beansprucht und bei Netzerweiterungen eine aufwendige Informationsübertragung verlangt, oder die Liste wird zentral geführt, was bei jedem Verbindungsaufbau zwei Rückfragen an die Schlüsselverteilzentrale verlangt.

Eine zentrale Liste mit lokalen Auszügen stellt für viele Anwendungen eine vernünftige Lösung dar. Dort wo jedoch die Verbindung bei wenig Speicherplatz, autonom aufgebaut werden soll und eine Authentifikation der Teilnehmer einzeln notwendig ist, ist auch dieses Verfahren nicht sehr hilfreich. Beispiele dafür sind Netze von POS-Terminals, mobile Telefonsysteme und sonstige Funknetze sowie Computernetze.

Zur Identifikation (u.a. an POS-Terminals) sind von

- Fiat und Shamir («How to Prove Yourself: Practical Solutions to Identification and Signature Problems», Advances in Cryptology – CRYPTO'86, Lecture Notes in Computer Science, Vol 263, pp. 186–194, Springer Verlag 1987),
- L.C. Guillou, J.-J. Quisquater («A Practical Zero Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory, Advances in Cryptology – EUROCRYPT'88, Lecture Notes in Computer Science, Vol 330, pp. 123–128, Springer Verlag 1988), und von
- T. Beth, («Efficient Zero Knowledge Identification Scheme for Smart Cards», Advances in Cryptology – EUROCRYPT'88, Lecture Notes in Computer Science, Vol. 330, pp. 77–84 Springer Verlag 1988)

sogenannte «zero knowledge proofs» vorgeschlagen worden. Bei einem solchen «zero knowledge proof» geht jeder Benutzer in einer Präauthentifikationsphase zur Schlüsselverteilzentrale, weist sich aus und bekommt von der Zentrale den öffentlichen Netzschlüssel sowie die zu seiner Identität ID (z.B. AHV-Nummer) gehörige Signatur S (ID), welche die Zentrale mit dem geheimen Netzschlüssel bildet.

Will sich nun A gegenüber einem anderen Benutzer B ausweisen, so beweist er in einem Protokoll mit B, dass er S(ID) kennt, ohne die Signatur selbst preiszugeben. Die Signatur wird dabei unter Verwendung des öffentlichen Netzschlüssels geprüft.

Darstellung der Erfindung

Aufgabe der Erfindung ist es, ein Verfahren zum authentifizierten Schlüsselaustausch in einem Netz mit einer Schlüsselverteilzentrale und mehreren Teilnehmern anzugeben, welches flexibel in bezug auf die Erweiterung durch neue Benutzer ist, einen geringen Speicherbedarf hat und die Nachteile der bekannten Verfahren vermeidet.

Erfindungsgemäss besteht die Lösung darin, dass in einer Präauthentifikationsphase

a) die Schlüsselverteilzentrale eine Funktion f(.) zur Erzeugung von Identitätsnummern, einen endlichen Körper GF(q), in welchem die Rechenoperationen ausgeführt werden, eine Funktion g: GF(q) x GF(q) → GF(q), ein primitives Element $\alpha \in GF(q)$ und eine geheime erste Zufallszahl x wählt, aus welchen sie einen öffentlichen Netzschlüssel $y = \alpha^{-x}$ bildet,

b) die Schlüsselverteilzentrale jedem Benutzer eine Identitätsnummer ID = f(A) signiert, indem die Schlüsselverteilzentrale eine geheime zweite Zufallszahl k wählt, welche die Eigenschaft gcd(k,q–1) = 1 hat, aus der Zufallszahl k einen öffentlichen Benutzerschlüssel $r = \alpha^k$ und einen geheimen Benutzerschlüssel s mit der Eigenschaft $xr+ks \equiv ID \bmod (q-1)$ bildet und dem Benutzer seine beiden Benutzerschlüssel mitteilt,

und dass in einer Schlüsselaustauschphase zwischen einem ersten Benutzer A und einem zweiten Benutzer B

c) jeder der beiden Benutzer A resp. B dem anderen seinen öffentlichen Benutzerschlüssel r resp. r' mitteilt,

d) jeder der beiden Benutzer A resp. B die Identitätsnummer ID' = f(B) resp. ID = f(A) bildet und aus dieser Identitätsnummer und dem Benutzerschlüssel r' resp. r des jeweils anderen eine Grösse $r's' = \alpha^{ID'}y^{r'}$ resp. $r^s = \alpha^{ID}y^r$ bildet,

e) jeder der beiden Benutzer A resp. B eine geheime Zufallszahl t resp. t' erzeugt und damit einen Code r^t resp. $r'^{t'}$ bildet, welchen er dem anderen Benutzer B resp. A mitteilt und

f) die beiden Benutzer A und B einen gemeinsamen geheimen Kommunikationsschlüssel

$z = g(r'^{s}, r^{s't})$ bilden.

Es versteht sich von selbst, dass der endliche Körper GF(q) so gewählt wird, dass q–1 eine Zahl mit mindestens einem grossen Primfaktor ist. Bis auf eine werden alle erfindungsgemässen Operationen in diesem Körper ausgeführt.

Mit den bekannten «zero knowledge proof» Verfahren hat die Erfindung die Eigenschaft gemeinsam, ebenfalls die Signatur der Identität S(ID) als

geheimes Authentifikationsmerkmal zu benutzen. Im Unterschied zu den bekannten Verfahren wird dieses Merkmal jedoch zur Konstruktion eines gemeinsamen, gegenseitig authentifizierten Schlüssels verwendet.

Aus den abhängigen Patentansprüchen ergeben sich vorteilhafte Ausführungsformen der Erfindung.

Kurze Beschreibung der Zeichnung

Nachfolgend soll die Erfindung anhand von Ausführungsbeispielen im Zusammenhang mit der Zeichnung näher erläutert werden. Es zeigen:

Fig. 1 eine schematische Darstellung der Präauthentifikationsphase; und

Fig. 2 eine schematische Darstellung der Schlüsselaustauschphase zwischen zwei Benutzern.

Die in der Zeichnung verwendeten Bezugszeichen und deren Bedeutung sind in der Bezeichnungsliste zusammenfassend tabelliert.

Wege zur Ausführung der Erfindung

Der erfindungsgemässe Schlüsselaustausch findet in einem für die Übertragung von digitalen Daten geeigneten Netz mit einer Schlüsselverteilzentrale SVZ und mehreren Benutzern A, B,... statt und weist zwei Phasen auf, nämlich eine Präauthentifikationsphase und eine Schlüsselaustauschphase. In der Präauthentifikationsphase kommt jeder Benutzer A, B,... zur Schlüsselverteilzentrale SVZ und lässt sich seine Identität gemäss dem El-Gamal-Schema signieren. In der nachfolgenden Schlüsselaustauschphase erzeugen zwei Benutzer A und B einen gemeinsamen Geheimschlüssel z nach einem abgeänderten Diffie-Hellmann-Verfahren.

Fig. 1 zeigt eine schematische Darstellung der Präauthentifikationsphase. Als erstes wählt (SELECT) die Schlüsselverteilzentrale SVZ einen endlichen Körper GF(q), wobei q–1 typischerweise einen grossen Primfaktoren aufweist, und ein primitives Element $\alpha \in GF(q)$. Dann erzeugt sie zufällig (RANDOM) als geheimen Netzschlüssel («private part») eine erste Zahl x, aus welcher sie einen öffentlichen Netzschlüssel («public part») $y = \alpha^{-x}$ bildet. (Es versteht sich, dass diese und die später beschriebenen Operationen im endlichen Körper GF(q) ausgeführt werden, wenn es nicht explizit anders spezifiziert wird.) Weiter definiert sie eine geeignete Funktion f(.), welche aus den Identitätsmerkmalen eine eindeutige Identitätsnummer erzeugt. Schliesslich definiert sie noch eine geeignete Funktion g: $GF(q) \times GF(q) \rightarrow GF(q)$. Vorzugsweise ist diese Funktion das Produkt.

Die durch f(.) bestimmte Identitätsnummer ID kann beispielsweise durch Abtasten des Fingers (Fingerabdruck) gebildet werden. Es können aber auch weitere Merkmale eingehen. Typischerweise ist f(.) eine Einwegfunktion (one way function), die auf den Datenstring bestehend aus Namen, Vornamen, Geburtsdatum und eventuell weiteren Merkmalen angewandt wird.

Den endlichen Körper GF(q), das primitive Element α und den öffentlichen Netzschlüssel y sowie die Funktion f(.) gibt die Schlüsselverteilzentrale SVZ öffentlich bekannt. Den geheimen Netzschlüssel x speichert sie zugriffsgeschützt ab.

Die Schlüsselverteilzentrale SVZ hat damit die grundlegenden, allgemeinen Vorbereitungen abgeschlossen. Nun kommt jeder Benutzer zur Schlüsselverteilzentrale SVZ und lässt sich seine Identität gemäss dem El-Gamal-Schema signieren.

Der Benutzer A weist sich aus (z.B. mit seinem Reisepass), worauf die Schlüsselverteilzentrale SVZ mit Hilfe der Funktion f(.) eine eindeutige Identitätsnummer $ID = f(A)$ berechnet. Dann erzeugt sie zufällig (RANDOM) eine benutzerspezifische Zahl k, welche die Eigenschaft $\gcd(k,q-1) = 1$ hat (gcd = greatest common divisor). Aus der zweiten Zufallszahl k bildet sie einen öffentlichen Benutzerschlüssel $r = \alpha^k$ und einen geheimen Benutzerschlüssel s mit der Eigenschaft $xr+ks = ID \bmod (q-1)$. Die beiden Benutzerschlüssel r und s teilt sie dem Benutzer A mit, der den geheimen Benutzerschlüssel s zugriffsgesichert abspeichert.

Jeder Benutzer, der im Netz zugelassen werden will, muss die beschriebene Präauthentifikationsphase durchlaufen.

Fig. 2 zeigt eine schematische Darstellung der Schlüsselaustauschphase. Sie findet zu Beginn einer Kommunikation zwischen einem ersten Benutzer A und einem zweiten Benutzer B statt.

Jeder der beiden Benutzer kennt dabei die öffentlich bekannten Parameter f(.), g(.,.), GF(q), α, y, sowie seine Schlüssel r und s resp. r' und s'. Typischerweise hat er auch seine eigene Identitätsnummer ID resp. ID' abgespeichert.

Die beiden Benutzer A und B berechnen als erstes die Identitätsnummer ID' und ID und tauschen den öffentlichen Benutzerschlüssel r und r' aus.

Als zweites bildet jeder der beiden Benutzer A resp. B aus der Identitätsnummer ID' resp. ID und dem Benutzerschlüssel r' resp. r des jeweils anderen eine Grösse $r'^{s'} = \alpha^{ID'y^{r'}}$ resp. $r^s = \alpha^{ID y^r}$. Als drittes erzeugen sie zufällig (RANDOM) je eine geheime Zahl t resp. t' und errechnen daraus je einen Code r^t resp. $r'^{t'}$. Dann wird dieser Code r^t resp. $r'^{t'}$ ausgetauscht. Zum Schluss bildet jeder der beiden Benutzer A resp. B aus den bekannten Grössen den gemeinsamen Geheimschlüssel («session key»)

$z = g(r'^s, r^{s't})$.

Das erfindungsgemässe Verfahren hat u.a. folgende Vorteile:

1. Ausser den eigenen Identifikationsmerkmalen genügt die Kenntnis eines einzigen «public keys» zum authentifizierten Schlüsselaustausch mit einem beliebigen anderen Benutzer des Netzes. Das Verfahren zeichnet sich folglich durch einen sehr geringen Speicherbedarf aus.

2. Jeder präauthentifizierte Benutzer kann mit jedem anderen präauthentifizierten Benutzer einen authentifizierten Schlüsselaustausch vornehmen, ohne dabei auf die Schlüsselverteilzentrale zurückgreifen zu müssen (off-line authentifizierter

Schlüsselaustausch). Ein mit diesem System betriebenes Netz ist dadurch auch beliebig flexibel in bezug auf Erweiterung des Teilnehmerkreises.

3. Dennoch sind bei dem erfindungsgemässen Schlüsselaustausch alle Teilnehmer unterscheidbar, d.h. es kann sich keiner für einen anderen ausgeben.

Zur Sicherheit des erfindungsgemässen Schlüsselaustausches lässt sich folgendes sagen:

1. Falls man s aus α, y, ID und r bestimmen kann, kann man das El-Gamal'sche Signaturschema brechen, welches allgemein als sicher angesehen wird.

2. Falls man $(r^{r'})^s$ aus r, r^s und $r^{r'}$ bestimmen kann, kann man den Diffie-Hellmann'schen Schlüsselaustausch-Algorithmus brechen, welcher ebenfalls allgemein als sicher angesehen wird.

Diese Überlegungen lassen es als wahrscheinlich erscheinen, dass bei geeigneter Wahl von q, α, x und k die Kenntnis von s resp. s' durch den Benutzer A resp. B unerlässlich ist für die Konstruktion des Sitzungsschlüssels z. Das erfindungsgemässe Schlüsselaustauschverfahren beinhaltet somit eine gegenseitige Authentifikation der Benutzer A und B.

Der resultierende Sitzungsschlüssel z kann nun für die verschiedensten Anwendungen benutzt werden, wie z.B. zur Chiffrierung, zur Sicherung der Datenintegrität oder auch nur zur Identitätskontrolle.

Das erfindungsgemässe Verfahren lässt sich mit als solchen bekannten Mitteln realisieren. Eine für den authentifizierten Schlüsselaustausch zwecks Chiffrierung geeignete Anordnung ist z.B. in der eingangs erwähnten deutschen Auslegeschrift DE-A 3 915 262 beschrieben.

Die Einsatzmöglichkeiten des beschriebenen Verfahrens sind aufgrund der erwähnten Vorteile ziemlich breit: Mobiles Telephon, Militärfunk, Computernetze und POS-Terminals.

Das beschriebene Schlüsselaustauschverfahren ist ein «public key» Verfahren mit einem einzigen Schlüssel, das einen authentifizierten Schlüsselaufbau zwischen zwei beliebigen Benutzern erlaubt. Es wird off-line betrieben, ist flexibel in bezug auf Erweiterungen durch neue Benutzer und hat einen geringen Speicherbedarf. Der Rechenaufwand ist im wesentlichen der gleiche wie beim weit verbreiteten Diffie-Hellmann-Verfahren. Die etwas aufwendigere El-Gamal Signatur wird jeweils von der Schlüsselverteilzentrale und ausserdem für jeden Benutzer nur einmal durchgeführt.

Patentansprüche

1. Verfahren zum authentifizierten Schlüsselaustausch in einem Netz mit einer Schlüsselverteilzentrale und mehreren Teilnehmern A, B, dadurch gekennzeichnet, dass in einer Präauthentifikationsphase

a) die Schlüsselverteilzentrale eine Funktion f(.) zur Erzeugung von Identitätsnummern, einen endlichen Körper GF(q), in welchem die Rechenoperationen ausgeführt werden, eine Funktion g: GF(q) x GF(q) $\rightarrow$ GF(q), ein primitives Element $\alpha \varepsilon$ GF(q) und eine geheime erste Zufallszahl x wählt, aus welchen sie einen öffentlichen Netzschlüssel $y = \alpha^{-x}$ bildet,

b) die Schlüsselverteilzentrale jedem Benutzer eine Identitätsnummer ID = f(A) signiert, indem die Schlüsselverteilzentrale eine geheime zweite Zufallszahl k wählt, welche die Eigenschaft gcd(k, q–1) = 1 hat, aus der Zufallszahl k einen öffentlichen Benutzerschlüssel $r = \alpha^k$ und einen geheimen Benutzerschlüssel s mit der Eigenschaft $xr+ks \equiv ID \bmod (q-1)$ bildet und dem Benutzer seine beiden Benutzerschlüssel mitteilt,

und dass in einer Schlüsselaustauschphase zwischen einem ersten Benutzer A und einem zweiten Benutzer B

c) jeder der beiden Benutzer A resp. B dem anderen seinen öffentlichen Benutzerschlüssel r resp. r' mitteilt,

d) jeder der beiden Benutzer A resp. B die Identitätsnummer ID' = f(B) resp. ID = f(A) bildet und aus dieser Identitätsnummer und dem Benutzerschlüssel r' resp. r des jeweils anderen eine Grösse $r^{s'} = \alpha^{ID'}y^{r'}$ resp. $r^s = \alpha^{ID}y^r$ bildet,

e) jeder der beiden Benutzer A resp. B eine geheime Zufallszahl t resp. t' erzeugt und damit einen Code r^t resp. $r^{t'}$ bildet, welchen er dem anderen Benutzer B resp. A mitteilt und

f) die beiden Benutzer A und B einen gemeinsamen geheimen Kommunikationsschlüssel $z = g(r^{t's}, r^{s't})$ bilden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Funktion g(.,.) die Multiplikation im endlichen Körper GF(q) ist.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Funktion f(.) eine Einwegfunktion ist.

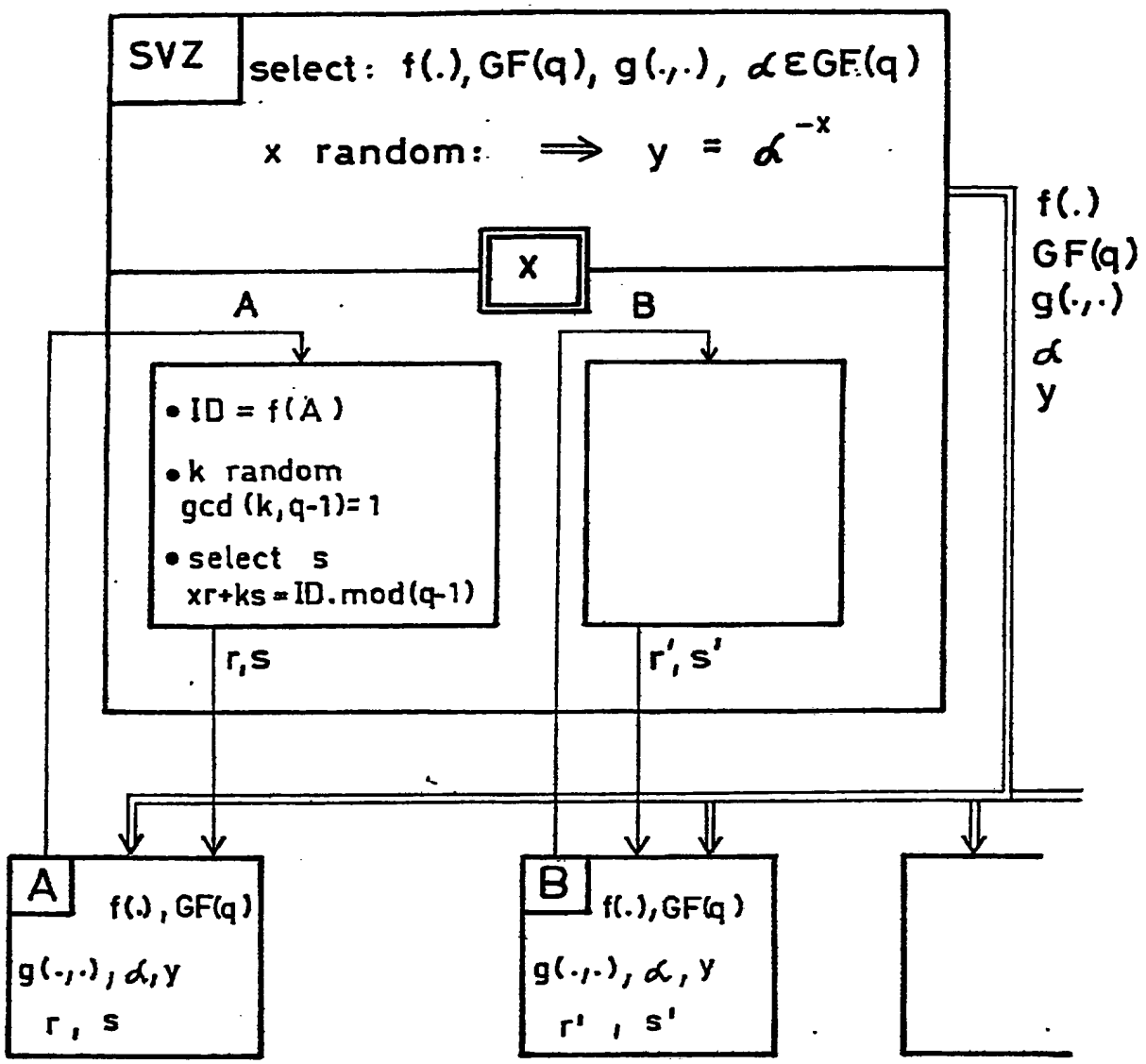

SVZ
select: f(.), GF(q), g(.,.), α ∈ GF(q)
x random: ⇒ y = α^-x
f(.)
GF(q)
g(.,.)
α
y
X
A
B
• ID = f(A)
• k random
gcd (k, q-1) = 1
• select s
xr+ks = ID. mod(q-1)
r, s
r', s'
A
f(.), GF(q)
g(.,.), α, y
r, s
B
f(.), GF(q)
g(.,.), α, y
r', s'

FIG.1

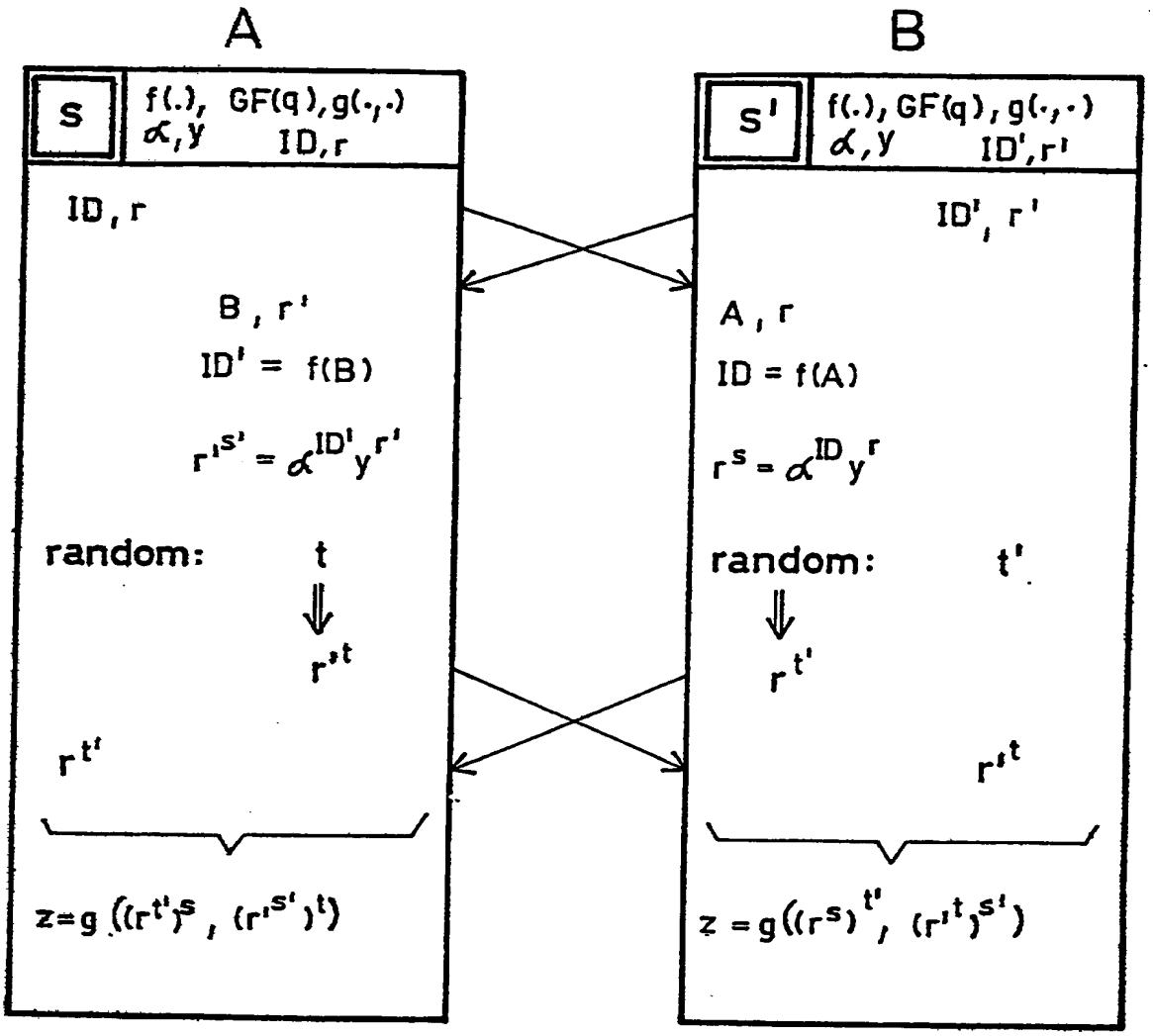

A
B
s
f(.), GF(q), g(·,·)
α, y
ID, r
s'
f(.), GF(q), g(·,·)
α, y
ID', r'
ID, r
ID', r'
B, r'
ID' = f(B)
A, r
ID = f(A)
random:
t
random:
t'
z=g((r^t')^s, (r'^s')^t)
z=g((r^s)^t', (r'^t)^s')

FIG.2